Rafey S. Balabanian (SBN 315962)
rbalabanian@edelson.com
Lily E. Hough (SBN 315277)
lhough@edelson.com
EDELSON PC
123 Townsend Street,
San Francisco, California 94107
Tel: 415.212.9300
Fax: 415.373.9435

Counsel for Plaintiff and the Putative Classes

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
OAKLAND DIVISION

S.D., individually and on behalf of all others similarly situated,

Plaintiff,

v.

HYTTO LTD., D/B/A LOVENSE, a Hong Kong, China corporation,

Defendant.

Case No. 4:18-CV-00688-JSW

PLAINTIFF'S OPPOSITION TO MOTION TO DISMISS

Judge: Hon. Jeffrey S. White

TABLE OF CONTENTS

TABLE OF AUTHORITIES

United States Supreme Court Cases

United States Courts of Appeals Cases

United States District Court Cases

Statutory Provisions

I. INTRODUCTION

Through its motion to dismiss (the "Motion"), Defendant Hytto Ltd. argues that the Court lacks personal jurisdiction over it and that Plaintiff cannot state a viable claim for relief. The Motion is most notable for what it ignores—namely, that Hytto's business unabashedly targets U.S. purchasers of its sex toys, and its "Body Chat App" (or "App"), which is a key part of those purchases, systematically captures and sends the intimate communications between "Long Distance" users of its products to Hytto. *Those* facts and allegations are critical to this case and, here, readily demonstrate that Hytto's Motion lacks merit on both fronts.

First, because this case centers on Plaintiff's claim under the federal Wiretap Act, Hytto is subject to specific jurisdiction pursuant to Rule 4(k)(2) of the Federal Rules of Civil Procedure. That conclusion follows because Hytto's alleged interceptions (*i.e.*, its unlawful capturing of communications between remote users of its sex toys, including Plaintiff) occurred within the U.S. and because Hytto directed claim-related conduct at the U.S. (including the programming and distribution of the App, along with its U.S.-targeted marketing efforts)

Second, Hytto fails to identify any basis for dismissal on the merits. For the Wiretap Act claim, Hytto emphasizes that its sex toys are controlled from users' phones via Bluetooth; but that strays far from Plaintiff's claim, which turns on the user-to-user communications sent over (and that could not have been sent without) the Internet. Next, Hytto says that the communications between users—"I want to vibrate your sex toy in this specific way"—aren't protected; but this confuses the content of users' communications (which are protected) with record information "about" those messages (which are not). And its final arguments about being a party to its customers' intimate communications and collecting those communications in the "ordinary course of business" have no basis in the pleadings, failing as a result. What's more, these same failings show that Plaintiff's intrusion upon seclusion claim should proceed as well.

II. BACKGROUND

Hytto is a Chinese company that markets and sells vibrators and other sex toys through its interactive website, which Hytto uses to target and attract customers in the United States. (Plaintiff's First Amended Complaint, "FAC" ¶¶ 6, 12–27.) This targeting is plain from the

commercial activities that take place on Hytto's website: the website provides ordering and shipping information for U.S. customers; calculates prices in U.S. dollars and accepts payments exclusively through PayPal, a U.S. company; displays text in English, including when users select a different language; relies on testimonials from U.S. customers; includes an interactive "Affiliate Program;" touts its "integration" with various U.S.-based companies; uses a ".com" suffix; and includes California-specific terms of use. (FAC ¶¶ 12–27.) (Declaration of Rafey S. Balabanian ("Balabanian Decl.") ¶¶ 5-7.) The results of this targeting are unsurprising. Recent data shows that U.S. users visit Hytto's website more than any other country (by far), and it has shipped a substantial amount of its products to U.S. customers. (Balabanian Decl. ¶¶ 2, 3.)

The defining feature of Hytto's sex toys is their "Long Distance Control" feature, which, through the Body Chat App, Defendant explains "allows you to give control to someone who is miles away . . . [and lets them] control your toy from THEIR phone." (FAC ¶ 32.) This functionality lets App users control each other's sex toys by sending commands over the Internet: a remote user can choose whether and how intensely to make their partner's device vibrate. (*Id.* ¶¶ 29–32.) Although Defendant promised that this remote connection is private and "peer-to-peer," it programmed the Body Chat App to re-route *all* vibrator control instructions—including ones that a user inputs herself *and* ones that she receives from remote partners over the Internet—to its own servers. (*Id.* ¶¶ 31–38.) Through this programming, Defendant captured information that identified its users *and* the specific instructions they inputted themselves (when operating their own sex toys) and/or exchanged with other users. (*Id.* ¶¶ 35–38.) Defendant did not seek consent from its users before capturing and collecting any of this data. (*Id.* ¶ 39.)

Plaintiff purchased a "Lush" vibrator from Defendant's website. (*Id.* ¶ 40.) She thereafter downloaded the App and used its Long Distance Control feature with a third party. (*Id.* ¶¶ 42, 44.) Each time Plaintiff used the vibrator in this fashion, Defendant intercepted the remote communications she received from the third party, and transmitted it to its own servers. (*Id.* ¶¶ 45–46.) Plaintiff never consented to this conduct and would not have purchased the Lush vibrator had she known of it at the time of her purchase. (*Id.* ¶¶ 47– 49.)

III. ARGUMENT

A. The Court Has Specific Personal Jurisdiction Over Defendant.

In contesting jurisdiction under Rule 4(k)(2), Defendant suggests that any sales of its sex toys to U.S. customers were fortuitous. The challenge ignores the pleadings almost entirely. Here, Plaintiff alleges the requisite minimum contacts for jurisdiction because Hytto committed tortious acts in the U.S. (the at-issue interceptions) *and* targeted the United States with its interactive website. Either set of allegations is sufficient to establish the Court's jurisdiction.

Under Rule 4(k)(2) a court may exercise personal jurisdiction if (i) a claim arises under federal law, (ii) defendant is not subject to general jurisdiction in any state, and (iii) doing so will not offend due process. Because no party requests an evidentiary hearing, Plaintiff must make a *prima facie* case of jurisdiction. *Schwarzenegger v. Fred Martin Motor Co.*, 374 F.3d 797, 800 (9th Cir. 2004). Jurisdictional allegations are accepted as true unless proven otherwise by affidavits or exhibits, and disputes are resolved in Plaintiff's favor. *Id.*

Here, the first Rule 4(k)(2) element is satisfied, as Plaintiff brings a claim under the federal Wiretap Act, and the Court's jurisdiction extends to Plaintiff's related state claims. *See Action Embroidery Corp. v. Atl. Embroidery, Inc.*, 368 F.3d 1174, 1181 (9th Cir. 2004) (adopting pendant personal jurisdiction doctrine). The second element is also satisfied, as Defendant has not identified any state where it is subject to general jurisdiction. *Holland Am. Line Inc. v. Wartsila N. Am., Inc.*, 485 F.3d 450, 461–62 (9th Cir. 2007). That leaves the due process inquiry, where Plaintiff must show Hytto has sufficient "minimum contacts" with the U.S. based on a three-part inquiry: (i) Defendant must have directed conduct at the U.S. or availed itself of the privilege of conducting activities here; (ii) the claim must arise from such conduct; and (iii) exercising jurisdiction must be reasonable. *Axiom Foods, Inc. v. Acerchem Int'l, Inc.*, 874 F.3d 1064, 1068 (9th Cir. 2017). Here, only the first two elements are at issue, and both are satisfied. [1]

1. Hytto's in-forum tortious conduct—its interceptions of Plaintiff's user-to-user communications—supports personal jurisdiction.

---

[1] Defendant bears the burden on the third prong, but makes no effort to lay out a "compelling case" that jurisdiction would be unreasonable. *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 243 F. Supp. 2d 1073, 1092 (C.D. Cal. 2003) (citing *Sinatra v. Nat'l Enquirer, Inc.*, 854 F.2d 1191, 1198-99 (9th Cir. 1988)). (*See* Mot. at 6 n. 4.)

While torts by foreign defendants are often analyzed using the purposeful direction inquiry, the Ninth Circuit recently emphasized that, in line with the purposeful availment analysis set out in *Paccar Int'l, Inc. v. Commercial Bank of Kuwait, S.A.K.*, 757 F.2d 1058 (9th Cir. 1985), "[t]he commission of an intentional tort in a [forum] is a purposeful act that will satisfy the first two requirements [of the minimum contacts test]." *Freestream Aircraft (Bermuda) Ltd. v. Aero Law Grp.*, No. 16-17347, 2018 WL 4440361, at *4 (9th Cir. Sept. 18, 2018) (internal quotation and citation omitted). This is true "even where the alleged tortfeasor is not physically present in that forum." *Apollo Educ. Grp., Inc. v. Somani*, No. C-15-1056 EMC, 2015 WL 4880646, at *3 (N.D. Cal. Aug. 13, 2015).

Here, because Hytto committed an international tort in the U.S.—the alleged interceptions underlying Plaintiff's Wiretap Act claim—it is subject to the jurisdiction of any U.S. court. *Freestream Aircraft*, 2018 WL 4440361, at *4; Fed. R. Civ. P. 4(k)(2). Plaintiff alleges that (i) Hytto distributed its products and the Body Chat App to its customers (including Plaintiff) in the U.S. and (ii) Hytto intercepted private communications each time those customers used the App's Long Distance Control feature with a remote partner in the United States.[2] (FAC ¶¶ 12, 16–18, 40–46.) *See Francis v. Api Tech. Servs., LLC*, No. 4:13-CV-627, 2014 WL 11462447, at *6 (E.D. Tex. Apr. 29, 2014), report and recommendation adopted, No. 4:13-CV-627, 2014 WL 11462449 (E.D. Tex. Sept. 11, 2014) (finding defendant "committed a tort in Texas" by "accessing [plaintiff's] private information without authorization"). Hytto's in-forum conduct therefore supplies the minimum contacts needed to establish personal jurisdiction.

2. Hytto purposefully directed its conduct and website at the U.S.

Hytto's out-of-forum conduct is also sufficient to establish personal jurisdiction under a purposeful direction analysis, which requires (i) an intentional act, (ii) expressly aimed at the

---

[2] What's more, the alleged interceptions would not have occurred but for other aspects of Hytto's in-forum conduct, through which it was able to sell, distribute, fund, and promote its products and App. (FAC ¶¶ 19 (use of U.S. partners to ship and store its products, and sells products in U.S. retail stores), 21 (funding achieved through U.S.-based partners and campaign), 24 (use of PayPal, a U.S. company, as exclusive online payment processor), 25–26 (use of U.S. companies to distribute App to U.S. customers), 22 (promotion of products through U.S. companies), 14–15 (establishing "affiliate" agreements with U.S. customers and partners).)

forum, (iii) causing harm the defendant knows is likely to be suffered in the forum. *Calder v. Jones*, 465 U.S. 783, 788 (1984). Express aiming" requires "a foreign act with foreseeable effects in the forum" plus "something more" such as widespread, repeated, or deliberate conduct. *See, e.g.*, *Pakootas v. Teck Cominco Metals, Ltd.*, No. 16-35742, 2018 WL 4372973, at *7 (9th Cir. Sept. 14, 2018) (express aiming where dumping of waste into Canadian river done with knowledge of downstream U.S. effects). Jurisdiction may arise from electronic contacts—even a single act, *Axiom Foods*, 874 F.3d at 1068—such as when a foreign party accesses a forum resident's emails or accesses forum-based servers. *See, e.g.*, *Francis*, 2014 WL 11462447, at *6 (accessing known forum resident emails was purposeful direction in Stored Communications Act case); *DEX Sys., Inc. v. Deutsche Post AG*, 727 F. App'x 276, 278 (9th Cir. 2018) (purposeful direction in copyright case where software used on servers in California).

Here, jurisdiction lies even if all of Hytto's relevant acts occurred outside the U.S. The first element of purposeful direction is satisfied, as Hytto effectively (and intentionally) distributed a "bug" to its customers: it programmed the App to capture communications between remote App users, and encouraged its customers to download and use it. (FAC ¶¶ 25–32, 35–39.) The final elements, express aiming and knowledge, are satisfied as well: Hytto knew Plaintiff (and tens of thousands of its other customers) lived in the U.S. and that its acts would result in the interception of user-to-user communications exchanged between App users in the forum. *Cf. Pakootas*, 2018 WL 4372973, at *7. Here, Plaintiff alleges that Hytto knew or should have known of the U.S. effects of its conduct for a number of reasons, including its shipment of a vibrator to Plaintiff's U.S. address to fill her online order and subsequent collection of "Plaintiff's personally identifiable Usage Information." (FAC ¶¶ 13, 40, 42–43, 45, 46.) This conduct was widespread. (*Id.* ¶¶ 35–39.) Finally, Plaintiff's Wiretap Act claim arises from Hytto's interception of U.S. residents' communications, facilitated through the App, which satisfies the second prong of the minimum contacts test.

If there were any doubt, Hytto's website readily provides the "something more" needed for jurisdiction. To evaluate purposeful direction based on a party's website, courts look at "the level of interactivity and commercial nature of the exchange of information that occurs on the

website to determine if sufficient contacts exist." *Craigslist, Inc. v. Kerbel*, No. 11–cv–3309–EMC, 2012 WL 3166798, at *4 (N.D. Cal. Aug. 2, 2012) (internal quotations omitted). Generally speaking, "[p]ersonal jurisdiction is appropriate where an entity is conducting business over the internet and has offered for sale and sold its products to forum residents." *Mysfyt, Inc. v. Lum*, No. 4:16-CV-03813-KAW, 2016 WL 6962954, at *3 (N.D. Cal. Nov. 29, 2016).

Here, the requirements for purposeful direction are met not just because the website is highly interactive, (*see* Mot. at 6), but because Hytto *intentionally* targeted the U.S. with its website and knew the effects of that targeting would be felt in the U.S. (FAC ¶¶ 35–39.) Numerous facts support this claim. On Lovense.com, Hytto "provides specific ordering information for [U.S.] customers," and lists the U.S. first in its country options for shipping purposes. (*Id.* ¶ 16; *see Graduate Mgmt. Admission Council v. Raju*, 241 F. Supp. 2d 589, 598 (E.D. Va. 2003) (website's "specific ordering information for [U.S.] customers" showed U.S.-targeting).) The website's Terms of Use and Privacy Policy have California-specific terms. (FAC ¶ 12; *see LiveCareer Ltd v. Su Jia Techs. Ltd.*, No. 14-CV-03336-JST, 2015 WL 1448505, at *4 (N.D. Cal. Mar. 31, 2015) (California-specific terms of use evidence of express aiming).) Hytto calculates purchases on its website in U.S. dollars and has customers make payments via PayPal. (FAC ¶¶ 16, 24; *see Quokka Sports, Inc. v. Cup Int'l Ltd.*, 99 F. Supp. 2d 1105, 1112 (N.D. Cal. 1999) (website's "pricing . . . in U.S. dollars" showed U.S.-targeting); *Professional's Choice Sports Med. Prods., Inc. v. Hegeman*, No. 15-CV-02505-BAS(WVG), 2016 WL 1450704, at *5 (S.D. Cal. Apr. 12, 2016) (the "use of Paypal demonstrates a high level of interactivity").) Hytto utilizes a ".com" domain name (rather than ".hk" for Hong Kong). (FAC ¶ 12.) Hytto's website displays text in English, even when a user selects a different language. (*Id.* ¶ 17.) Most of the customer testimonials on Lovense.com are from U.S. customers. (*Id.* ¶ 18; Balabanian Decl. ¶ 5, Ex. D; see *Raju*, 241 F. Supp. 2d at 598-99 (testimonials from U.S. citizens reflect U.S.-targeting).) The website also explicitly notes that the products are "integrated" with various U.S.-based companies. (Balabanian Decl ¶ 6, Ex. E.) *See Quokka Sports*, 99 F. Supp. 2d at 1112 (website's banner ads by U.S. businesses reflect U.S.-targeting). Finally, Hytto's website directs visitors to its Affiliate Program, a highly interactive feature that allows consumers to earn

commissions promoting Hytto's products—using links and banner ads created by Hytto—where the ads are in English and the commissions are calculated in U.S. dollars (regardless of the language settings on the website); unsurprisingly, persons in the U.S. participate in the Affiliate Program. (FAC ¶¶ 14–15, 17; Balabanian Decl ¶ 3, Ex. B; *see Metro-Goldwyn-Mayer*, 243 F. Supp. 2d at 1087 (factors showing website targeting include "whether the defendant exchanged messages with forum residents or gained subscribers through its contacts").) Hytto calls these contacts "random" or "fortuitous." (Mot. at 7.) On the contrary, they show both Hytto's online interactivity with the U.S. and its intentional targeting of the U.S. market.

The results of this targeting also support jurisdiction. The U.S. has made up the largest share of Lovense.com's web traffic in the past 6 months alone. (Balabanian Decl. ¶ 4, Ex. C; *Mavrix Photo, Inc. v. Brand Techs., Inc.*, 647 F.3d 1218, 1230 (9th Cir. 2011) ("substantial number of hits" on website from forum help establish personal jurisdiction).) Further, jurisdictional discovery confirmed that Hytto maintains a broad U.S. consumer base. In 2016–17, Hytto shipped nearly 100,000 products to the U.S.; saw 34,076 U.S. consumers download its App; and received over $14 million in revenue from U.S. sales. (Balabanian Decl. ¶¶ 2-3, Exs. A, B.) Such extensive commercial activity with the U.S., combined with electronic activity specifically directed at U.S. consumers, is enough to find that Hytto expressly aimed sales at the U.S market, and knew that any harm caused by such sales would be felt in the U.S. *See, e.g.*, *Mavrix Photo*, 647 F.3d at 1230 (express aiming where website's audience in the forum "an integral component of [Defendant's] business model and its profitability"); *D.light Design, Inc. v. Boxin Solar Co.*, No. 13-CV-05988-EMC, 2015 WL 7731781, at *2 (N.D. Cal. Dec. 1, 2015) (collecting cases where personal jurisdiction found for "defendants who conduct interactive online activities with forum residents or direct business to the forum"). And because the interception at issue would not have occurred but for Hytto's online efforts (*i.e.*, it "arises from" the conduct), (FAC ¶¶ 21–32), Hytto's connection with the U.S. demonstrates the required minimum contacts to exercise personal jurisdiction over it.

B. Plaintiff States a Claim Under the Federal Wiretap Act.

The Wiretap Act makes it unlawful to "intentionally intercept[] . . . any wire, oral, or

electronic communication."18 U.S.C. § 2511(1)(a). Plaintiff alleges that Defendant used its Body Chat App to continuously and contemporaneously intercept the remote vibrator control instructions she received over the internet from a third-party App user. That interception readily sets out a claim for unlawful interception under the Wiretap Act.

A complaint survives a Rule 12(b)(6) motion to dismiss when it contains "enough facts to state a claim for relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). Detailed factual allegations are not required, and "[a] claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). In evaluating a defendant's Rule 12(b)(6) motion, a court construes the complaint in the light most favorable to the plaintiff, accepting all well-pleaded facts as true, and drawing all reasonable inferences in the plaintiff's favor. *See Dahlia v. Rodriguez*, 735 F.3d 1060, 1066 (9th Cir. 2013). "On a motion to dismiss, facts outside the pleadings will not be considered." *Fields v. Wise Media LLC*, No. C 12-05160 WHA, 2013 WL 12174296, at *5 (N.D. Cal. Jan. 25, 2013).[3]

Defendant's bid for dismissal centers on four arguments. It says dismissal is warranted because (i) its products were controlled locally via Bluetooth, which does not implicate interstate commerce; (ii) the communications exchanged lack any "content;" (iii) it is a party to every communication between App users; and (iv) the interceptions happened in the ordinary course of business and fall under a Wiretap Act exception. As discussed below, each challenge fails.

---

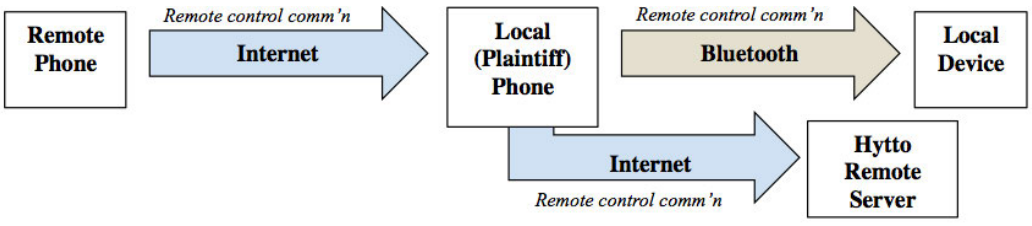
[3] The Motion's use of extrinsic information sources to support its Rule 12(b)(6) arguments should be rejected. For example, Hytto cites a webpage from Apple's iTunes store, (Mot. at 2 n.2), but that webpage (which discusses the *current* version of the Body Chat App, which may or may not have any bearing on the version that Plaintiff used) is not referenced in or incorporated by the FAC. It also cites a paper written by Joshua Wright, suggesting the contents are "scientific facts" that are "well established and generally acceptable." (Mot. at 3 n.2.) But again, the paper is not referenced by the FAC and there is no basis to evaluate the extrinsic evidence offered by Hytto, which—at best—may be a subject for expert testimony later in the case. Relatedly, Hytto cites documentation regarding how iOS and Android devices use Bluetooth. (Mot. at 3 n.3.) This is also improper; there is no showing that these materials governed the coding and operation of the App when the App was developed/deployed, or that they applied to the version of iOS used by Plaintiff (which isn't identified in the FAC). As such, their application here is subject to reasonable dispute and, thus, the Court should decline to take judicial notice of them.

1. The remote user-to-user communications were made via the Internet and therefore affected interstate commerce.

Defendant contends that because the user-to-user communications at issue are ultimately used to operate a Bluetooth-connected sex toy, they are "local" in nature and cannot form the basis of a claim under the Wiretap Act. (Mot. at 9.) This attempt to re-cast Plaintiff's claim must be rejected. The case is about Defendant's interception of *remote* communications exchanged between Body Chat App users. Because those communications could only be made over the internet (and were captured by Defendant contemporaneously with their transmission and receipt), they unquestionably involve a system affecting interstate commerce.

The Wiretap Act prohibits the interception of "electronic communications" "transmitted in whole or in part by a . . . system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12) (emphasis added). Where a communication is transmitted "through the internet . . . the [Wiretap Act's] interstate commerce requirement will have been met." *McCann v. Iroquois Mem'l Hosp.*, 622 F.3d 745, 752 n. 1 (7th Cir. 2010). *See also U.S. v. Sutcliffe*, 505 F.3d 944, 952 (9th Cir. 2007) ("[U]se of the internet is intimately related to interstate commerce.").

Here, the Wiretap Act claim is based on Defendant's interception of internet-based communications. Plaintiff alleges that, through the Body Chat App, users could "use[] the internet" to control Lovense devices "over long distances" and from "remote locations." (FAC ¶ 30.) When using the App's "Long Distance Control" with a remote partner, Plaintiff's phone functioned as a pass-through between her partner's device and her own, with Defendant intercepting the message as it passed from the remote user, through her phone, and onto her sex toy (and, thanks to its ongoing interception scheme, Defendant's remote servers):



(*See* FAC ¶¶ 29–30, 35–37.) Because this pathway *could not function* without an active internet connection, it necessarily utilizes a system affecting interstate commerce. (*Id.*)

Defendant tries to equate the App's Long Distance Control functionality with

"keylogger" software, which captures keystrokes as a user types them on a keyboard, (Mot. at 9), but the comparison doesn't hold up. Many courts have noted that keylogger software functions on a closed, offline system: the software registers keystrokes and nothing more. *See, e.g., U.S. v. Ropp*, 347 F. Supp. 2d 831, 837-38 (C.D. Cal. 2004). Thus, even if a keylogger captures information as it's entered onto a website, the "network connection is irrelevant" because the recorded keystrokes "could have been made on a stand-alone computer that had no link at all to the internet or any other external network." *Id.*; *accord Rene v. G.F. Fishers, Inc.*, 817 F. Supp. 2d 1090, 1094 (S.D. Ind. 2011) ("The key to the *Barrington* decision lies in the fact that the transmission of keystrokes exists internally on a computer. The relevant 'interception' acted on a system that operated solely between the keyboard and the local computer[.]").[4] Here, while a user's local control of his or her own Lovense device could be done using his or her own phone and a Bluetooth connection (and, presumably, without an internet connection), the Long Distance Control communication *requires* an internet connection and, by design, travels on a system affecting interstate commerce. *Id.* Indeed, even if discovery reveals that Defendant's interceptions occurred as a local App user's phone passes remote instructions to a Lovense device—akin to how webpage data received by a computer is passed to and rendered on a user's screen—the claim can proceed. *See, e.g., Shefts v. Petrakis*, No. 10-CV-1104, 2012 WL 4049484, at *8 (C.D. Ill. Sept. 13, 2012) (distinguishing keylogger cases and finding that software that took screenshots of information appearing on plaintiff's computer screen (i.e., *after* the transmitted information had been received over the internet) allowed defendants to view plaintiff's "communications as they were transmitted between his computer and others across the internet"); *Potter v. Havlicek*, No. 3:06-CV-211, 2007 WL 539534, at *7 (S.D. Ohio Feb. 14, 2007) ("In contrast to . . . keystrokes, which, when recorded, have not traveled in interstate

[4] Defendant's treatment of *Rene* and *Ropp* is misleading. (Mot. at 10–11.) As discussed herein, the reason that keylogger cases often don't state claims under the Wiretap Act is that the "intercepted" communications consist only of a local user typing away on his local keyboard: the software doesn't care if the computer is or is not connected to the internet, and it certainly can't capture *incoming* communications. Here, in contrast, the Long Distance Control feature *could not function* without the internet (there's no other way for a local user's App to receive a remote command) and, unlike the capturing of local keystrokes, the Defendant intercepted *incoming* communications from remote users contemporaneous with their arrival on Plaintiff's phone.

commerce, the incoming emails subjected to the screen shot software have traveled in interstate commerce."); *cf. Cline v. Reetz-Laiolo*, No. 3:17-CV-06866-WHO, 2018 WL 3159248, at *31 (N.D. Cal. June 28, 2018) (denying motion to dismiss and noting that resolution of the plaintiff's Wiretap Act claim, which turned on defendant's installation of software that collected keystrokes and screenshots, would depend on "the precise nature of the software [at issue].").

2. Plaintiff's Wiretap Act claim is not based on record information "about" her user-to-user communications.

Next, Defendant suggests that it did not intercept any message "content" because the communications sent from remote users "lack[] words and any intended message." (Mot. at 11.) The argument badly misconstrues applicable law and fails as a result.

The Wiretap Act prohibits the "acquisition of the contents of any" electronic communication. 18 U.S.C.A. §§ 2510(4), 2511(1). The Act defines "contents" as "any information concerning the substance, purport, or meaning that of [a] communication." 18 U.S.C. § 2510(8). The "content" of a message is information "generated . . . through the intent of the user." *Yunker v. Pandora Media, Inc.*, No. 11-CV-03113 JSW, 2013 WL 1282980, at *6–7 (N.D. Cal. Mar. 26, 2013). A message's content needn't be expressed in words. *See, e.g., Rainsy v. Facebook, Inc.*, 311 F. Supp. 3d 1101, 1115 (N.D. Cal. 2018) (finding that a Facebook "like" is "content" under 18 U.S.C. § 2510(8)); *see also Gonzales v. Uber Techs., Inc.*, 305 F. Supp. 3d 1078, 1085 (N.D. Cal. 2018), *on reconsideration*, No. 17-CV-02264-JSC, 2018 WL 3068248 (N.D. Cal. June 21, 2018) (price of an Uber ride communicated from a driver would be "content" protected by the Wiretap Act, if a driver "intended to communicate" it). While the Wiretap Act protects the contents of communications, it does not protect "record information regarding the characteristics of the message that is generated in the course of the communication," such as a phone call's "origin[], length, and time." *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014) (citing *U.S. v. Reed*, 575 F.3d 900, 917 (9th Cir. 2009)).

Here, Plaintiff alleges that Defendant captured both automatically generated "record information" (*e.g.*, the date and time of a particular message, (FAC ¶ 36)), along with the *intended content* of those users' communications, such as whether and how to control their

partners' Lovense devices, (*id.* ¶¶ 36–37). It is the interception of the intentional content between App users—"I want to cause your sex toy to vibrate at this intensity level"—that implicates the Wiretap Act. *See Yunker*, 2013 WL 1282980, at *6–7.

Defendant writes these communications off as "transactional records generated when the App controls the settings on the vibrator." (Mot. at 12.) If Plaintiff's claim were just about her *own* use and control of her vibrator, Defendant may have a point; her local use of a vibrator may be no different than setting "the speed of [her own] ceiling fan"—at least for the purposes of the Wiretap Act. (*Id.* at 11.) But here, Defendant was not watching Plaintiff use the "+ or – button on [her own vibrator]," (*id.* at 12); it was monitoring the decisions that "Long Distance" App users make about how to operate their *partners'* sex toys. Such monitoring involved Defendant's unlawful interception of the intended content of communications between remote App users.

3. Defendant is not a party to communications between remote App users.

Defendant suggests that it cannot be liable under the Act because its App facilitates the transmission of vibration instructions from a user's phone to the vibrator, which makes Defendant "the sender of the communication" and party to the intimate interactions between Plaintiff and her remote partner. (Mot. at 13.) The argument is wrong—not to mention creepy.

It's commonsense that a party to a communication cannot "intercept" it. In *Crowely v. CyberSource Corp., et al.*, cited by Hytto, the plaintiff alleged he "sent certain information [via email over the internet] to Amazon." 166 F. Supp. 2d 1263, 1269 (N.D. Cal. 2001). The Court had little trouble concluding that Amazon's receipt of the email was not an "interception" under the Wiretap Act. *Id.*; *cf. U.S. v. Pasha*, 332 F.2d 193, 198 (7th Cir. 1964) (officer's act of answering a telephone call (by picking up a ringing receiver) was not an "interception").

There are no analogous allegations here. The idea that remote App users intentionally invited Hytto into their intimate "long distance relationships," (FAC ¶ 31), is patently absurd. Defendant cites no authority suggesting that because its App facilitates the *remote* communications at issue, means that it is a "party" to those communications anymore than Apple is a party to every communication made using one of its iPhones, or Facebook is a party to every

message sent between its users. *See generally, e.g.*, *Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 846 (N.D. Cal. 2014); *Backhaut v. Apple, Inc.*, 74 F. Supp. 3d 1033, 1044 (N.D. Cal. 2014).

Hytto's reliance on internet "cookie" cases is misplaced. In *In re Google Cookie, Inc. Placement Consumer Privacy Litigation*, the plaintiffs alleged that Google "intercepted" information sent to websites using cookies, which tracked their browsing history. 806 F.3d 125, 140 (3d Cir. 2015), *cert. denied sub nom. Gourley v. Google, Inc.*, 137 S. Ct. 36 (2016). But browser cookies, by design, do not "intercept" anything (technically or legally). Rather, when a user requests the content of a webpage using an internet browser, multiple, independent requests for information are transmitted: the user's browser will send "GET" requests both to the owner of the webpage and, through embedded browser cookies, to other parties (including Google) for advertising content associated with that webpage. *Id.* at 141. Because the plaintiffs made simultaneous requests for content directly to website operators *and* Google, the Third Circuit found no interception occurred because "the plaintiffs' browsers [acting on behalf of the plaintiffs] sent that information directly to [Google's] servers." *Id.* at 142; *accord In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 274 (3d Cir. 2016) (following *In re Google Cookie Placement* in finding that "Google was . . . a party to all communications with the plaintiffs' computers[.]"). Here, the communications at issue are those between Plaintiff and her remote partner; there was no "additional" communication between Plaintiff (or her partner) and Defendant.

4. No facts support applying the Wiretap Act's ordinary course of business exception.

Finally, Hytto raises a threadbare argument that its interception of remote App users' communications triggers the Wiretap Act's ordinary course of business exception, because "Hytto's collection of Usage Information facilitates [the sex toy's ability to be controlled by the App.]" (Mot. at 14.) Defendant, however, cites nothing to support its conclusory claim of "facilitation." The argument fails as a result.

As it applies to providers, (*see* Mot. at 14), the Wiretap Act's ordinary course of business exception is narrow, and applies where the alleged interceptions "facilitate[] the transmission of

the communication at issue or is incidental to the transmission of such communication." *In re Google Inc.*, No. 13-MD-02430-LHK, 2013 WL 5423918, at *8 (N.D. Cal. Sept. 26, 2013). Accordingly, there "must be some nexus between the need to engage in the alleged interception and the [provider's] ultimate business, that is, the ability to provide the underlying service or good." *Matera v. Google Inc.*, No. 15-CV-04062-LHK, 2016 WL 8200619, at *7 (N.D. Cal. Aug. 12, 2016) (quoting *In re Google*, 2013 WL 5423918, at *11). The fact that a defendant's collection or interception of data is "related" to its business—*e.g.*, "is in the service of making money"—is insufficient, as it would let companies "self-define the scope of the exception." *Campbell*, 77 F. Supp. 3d at 844.

Here, there are no allegations addressing why Hytto captures Usage Information—much less ones showing that Defendant's collection of the data was necessary to "facilitate" the Long Distance Control feature. (*See generally* FAC.) Without support, argument fails. *See Campbell*, 77 F. Supp. 3d at 844 ("Based on the current record, the court cannot find any facts alleged in the complaint or facts presented by Facebook that indicate a nexus between Facebook's alleged scanning of users' private messages for advertising purposes and its ability to provide its service."); *see also Dunbar v. Google, Inc.*, No. 5:10-CV-194-DF, 2011 WL 12907501, at *4 (E.D. Tex. May 23, 2011) (finding "[t]he applicability of the 'ordinary course of business' exception therefore cannot be resolved at the pleading stage."). Besides, Plaintiff alleges the interceptions were contrary to Defendant's data transmission practices (which were described as "peer-to-peer," (FAC ¶ 33)), cutting against any application of the ordinary course of business exception. *See, e.g., In re Google*, 2013 WL 5423918, at *12 (allegations that defendant's data collection "violate[d] its own policies [and thus acted] outside the ordinary course of business.").

C. Plaintiff States a Claim for Intrusion Upon Seclusion.

Defendant raises cursory arguments against Plaintiff's common law claim for intrusion upon seclusion, but fails to identify a basis for dismissal.

Plaintiff's intrusion upon seclusion claim is based on Defendant's practice of capturing incredibly intimate information about when and how Plaintiff used her vibrator, either by herself or with a remote party. *Cf. Witt v. Dep't of Air Force*, 527 F.3d 806, 813 (9th Cir. 2008)

("[Sexual behavior is] the most private human conduct") (quoting *Lawrence v. Tex.*, 539 U.S. 558, 567 (2003)). Hytto seeks dismissal, suggesting that it "was a party to the communication[s]" when remote App users control each other's (or their own) vibrators. (Mot. at 14-15.) But as discussed, the contention is a false one. (*Supra* § III.B.3.) For similar reasons, *Robinson v. Renown Regional Medical Center* offers no assistance to Hytto either. There, the Court found there was no intrusion upon information that the plaintiff provided to a third party, who then disclosed it onto the defendant. *Robinson*, No. 16-cv-372, 2016 WL 7031910, at *4 (D. Nev. Aug. 23, 2016). Here, neither Plaintiff nor her remote partner is alleged to have disclosed their use and control of Plaintiff's vibrator to any third party. Indeed, the only "disclosure" occurred as a result of the transmissions effectuated by Hytto, where it obtained information about Plaintiff's uses of her vibrator, including when she used it with a remote party.

Finally, Hytto cites cases generally discussing the idea that if a user wants to keep web browsing private, she may take steps to do so. *See In re Facebook Internet Tracking Litig.*, 263 F. Supp. 3d 836, 846 (N.D. Cal. 2017). Hytto stretches the holding of these cases too far: they do not stand for the proposition that the user of a mobile app should assume all activity is tracked and sent to third parties—particularly here, where Defendant advertised that all communications through the device would be secure and peer-to-peer, only. (FAC ¶ 31–34.) And besides, Plaintiff wasn't playing Angry Birds; she was using the App to control her vibrator. Suggesting that she had no expectation of privacy in how she used *this* App defies common sense. [5]

IV. CONCLUSION

For the reasons discussed herein, Defendant's Motion should be denied.

Respectfully submitted,

S.D., individually and on behalf of all others similarly situated,

[5] While Plaintiff states a claim for unjust enrichment under Georgia law based on her payment for—but failure to receive—a *secure*, "peer-to-peer" device, *see Clark v. Aaron's, Inc.*, 914 F. Supp. 2d 1301, 1309 (N.D. Ga. 2012), she acknowledges that the FAC does not explicitly identify any state's law in the unjust enrichment count and seeks leave to re-plead the claim.

Dated: October 11, 2018

By: /s/ Rafey S. Balabanian
One of Plaintiff's Attorneys

Rafey S. Balabanian (SBN 315962)
rbalabanian@edelson.com
Lily E. Hough (SBN 315277)
lhough@edelson.com
EDELSON PC
123 Townsend Street, Suite 100
San Francisco, California 94107
Tel: 415.212.9300
Fax: 415.373.9435

Counsel for Plaintiff and the Putative Classes

FILER'S ATTESTATION

I, Rafey S. Balabanian, am the ECF user whose identification and password are being used to file this Notice of Amendment Pursuant to Rule 15(a)(2). I hereby attest that all signatories listed on the preceding page concur in this filing.

Dated: October 11, 2018 /s/ Rafey S. Balabanian